Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 4/22

(Certification No.)

Prodotto: *(Product)* **Kaspersky Endpoint Security for Windows (version 11.6.0.394 AES256)**

Sviluppato da: *(Developed by)* **AO Kaspersky Lab**

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

The product identified in this certificate complies with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:

EAL2+
(ALC_FLR.1)

Il Direttore
(Dott.ssa Eva Spina)

[ORIGINAL DIGITALLY SIGNED]

Roma, 26 gennaio 2022

Common Criteria

SOGIS IT SECURITY CERTIFIED

This page is intentionally left blank

Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Certification Report

Kaspersky Endpoint Security for Windows (version 11.6.0.394 AES256)

OCSI/CERT/CCL/02/2021/RC

Version 1.0

26 January 2022

Courtesy translation

Disclaimer: this translation in English language is provided for informational purposes only; it is not a substitute for the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	26/01/2022

2 Table of contents

3 Acronyms

AES	Advanced Encryption Standard
AV	Anti-Virus
CB	Certification Body
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
CPU	Central Processing Unit
DLL	Dynamic-link library
DPCM	Decreto del Presidente del Consiglio dei Ministri
DRBG	Deterministic Random Bit Generator
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FDE	Full Disk Encryption
GB	Gigabyte
GHz	Gigahertz
HMAC	Keyed-Hash Message Authentication Code
IT	Information Technology
KES	Kaspersky Endpoint Security
KSC	Kaspersky Security Center
LAN	Local Area Network
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
NIST	National Institute of Standards and Technology
OCSI	Organismo di Certificazione della Sicurezza Informatica

OS	Operating System
PBKDF2	Password-Based Key Derivation Function 2
PP	Protection Profile
RAM	Random Access Memory
RSA	Rivest, Shamir, Adleman
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SIMD	Single Instruction stream, Multiple Data stream
SOGIS-MRA	Senior Officials Group Information Systems Security – Mutual Recognition Arrangement
SSE	Streaming SIMD Extensions
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
XML	Extensible Markup Language
XXE	XML External Entity

4 References

4.1 Criteria and regulations

[CC1] CCMB-2017-04-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2017-04-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2017-04-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 5, April 2017

[CC-STL] CCDB-2006-04-004, “ST sanitising for publication”, April 2006

[CCRA] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, July 2014

[CEM] CCMB-2017-04-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 5, April 2017

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

[SOGIS] “Mutual Recognition Agreement of Information Technology Security Evaluation Certificates”, Version 3, January 2010

4.2 Technical documents

[ETR] “Kaspersky Endpoint Security for Windows (version 11.6.0.394 AES256)” Evaluation Technical Report, v1, CCLab Software Laboratory, 6 December 2021

[KESUM] “Kaspersky Endpoint Security for Windows. User Manual”, Version 2.01, AO Kaspersky Lab

[KESUMA] “Kaspersky Endpoint Security for Windows. User Manual. Addendum A”, Version 2.04, AO Kaspersky Lab, 26 November 2021

[KESPP] “Kaspersky Endpoint Security for Windows. Preparative Procedures”, Version 2.03, AO Kaspersky Lab, 26 November 2021

[ST] “Kaspersky Endpoint Security for Windows. Security Target”, Version 2.04, AO Kaspersky Lab, 26 November 2021

[ST-LITE] “Kaspersky Endpoint Security for Windows. Security Target Lite”, Version 2.04, AO Kaspersky Lab, 26 November 2021 (sanitised public document)

5 Recognition of the certificate

5.1 European Recognition of CC Certificates (SOGIS-MRA)

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA, version 3 [SOGIS]) became effective in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) Evaluation Assurance Level up to and including EAL4 for all IT-Products. A higher recognition level for evaluations beyond EAL4 is provided for IT-Products related to specific Technical Domains only.

The current list of signatory nations and of technical domains for which the higher recognition applies and other details can be found on https://www.sogis.eu/.

The SOGIS-MRA logo printed on the certificate indicates that it is recognized under the terms of this agreement by signatory nations.

This certificate is recognized under SOGIS-MRA for all declared assurance components.

5.2 International recognition of CC certificates (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA] has been ratified on 08 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on https://www.commoncriteriaportal.org/.

The CCRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under CCRA for all declared assurance components.

6 Statement of certification

The Target of Evaluation (TOE) is the product “Kaspersky Endpoint Security for Windows (version 11.6.0.394 AES256)”, also referred to in the following as “KES”, developed by AO Kaspersky Lab.

The TOE is a software product that provides wide range of cybersecurity functionality for the endpoint devices, such as encryption of device data, anti-virus, and access control. Together with the Kaspersky Security Center (KSC), a centralised management console, KES builds a cybersecurity suite for protection of personal computer systems using Windows as operating system.

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3]. The Scheme is operated by the Italian Certification Body “Organismo di Certificazione della Sicurezza Informatica (OCSI)”, established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [ST]; the potential consumers of the product should review also the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC v 3.1 for the assurance level EAL2, augmented with ALC_FLR.1, according to the information provided in the Security Target [ST] and in the configuration shown in Annex B – Evaluated configuration of this Certification Report.

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA] and that no exploitable vulnerability was found. However, the Certification Body with such a document does not express any kind of support or promotion of the TOE.

A Security Target Lite [ST-LITE] is provided for publication. It is a sanitised version of the Security Target [ST] used for the evaluation, with removal of confidential proprietary technical information. Sanitisation was performed according to the rules outlined in the relevant CCRA supporting document [CC-STL].

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product “Kaspersky Endpoint Security for Windows (version 11.6.0.394 AES256)” to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should review also the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	Kaspersky Endpoint Security for Windows (version 11.6.0.394 AES256)
Security Target	“Kaspersky Endpoint Security for Windows. Security Target”, Version 2.04 [ST]
Evaluation Assurance Level	EAL2 augmented with ALC_FLR.1
Developer	AO Kaspersky Lab
Sponsor	AO Kaspersky Lab
LVS	CCLab Software Laboratory
CC version	3.1 Rev. 5
PP conformance claim	No compliance declared
Evaluation starting date	11 May 2021
Evaluation ending date	6 December 2021

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [ST] are fulfilled.

7.3 Evaluated product

This section summarizes the main functional and security requirements of the TOE. For a detailed description, please refer to the Security Target [ST].

The TOE “Kaspersky Endpoint Security for Windows (version 11.6.0.394 AES256)” is a software product that provides a wide range of cybersecurity functionality for the endpoint devices, such as encryption of device data (user data, operating system data), anti-virus, and access control. Together with the Kaspersky Security Center (KSC), a centralized management console, KES builds a cybersecurity suite for protection of personal

computer systems (work stations, laptops and other devices) using Windows as operating system.

KES combines anti-malware with application startup control, device access control, and web access control, plus data encryption in a single application.

The Full Disk Encryption (FDE) functionality helps protecting valuable business data from accidental loss due to lost or stolen devices.

The main functionalities of the evaluated TOE are the following:

- Anti-Virus protection:
  - File system protection
  - Network protection and traffic scanning
  - Proactive Defense
- Controls:
  - Application Startup Control
  - Device Access Control
  - Web Access Control
- Full Disk Encryption
- Management of all above, including user identification and authentication

For a detailed description of the TOE, consult sects. 1.3 and 1.4 of the Security Target [ST]. The most significant aspects are summarized below.

7.3.1 TOE architecture

The TOE consists of the following subsystems:

- **FDE subsystem**: this subsystem provides mechanisms to prohibit the access to the device data and cryptographic keys from an unauthorized individual who has physical access to the switched off device. This subsystem enforces all cryptography-related functionality and provides OS with ability to conduct read/write operation on encrypted disk(s). It requires each user to be successfully identified and authenticated before invoking security functionality responsible for transparent decryption of encrypted disk(s). This subsystem provides authorized users with ability to change their password.

- **KES subsystem**: this subsystem enforces the device access and application control policy using securely configurable rules. KES maintains the roles of KLUser and KLAdmin and is able to associate particular users with them. KES requires each user to be successfully identified and authenticated before invoking security functionalities.

The overview of the TOE physical architecture is given in Figure 1.

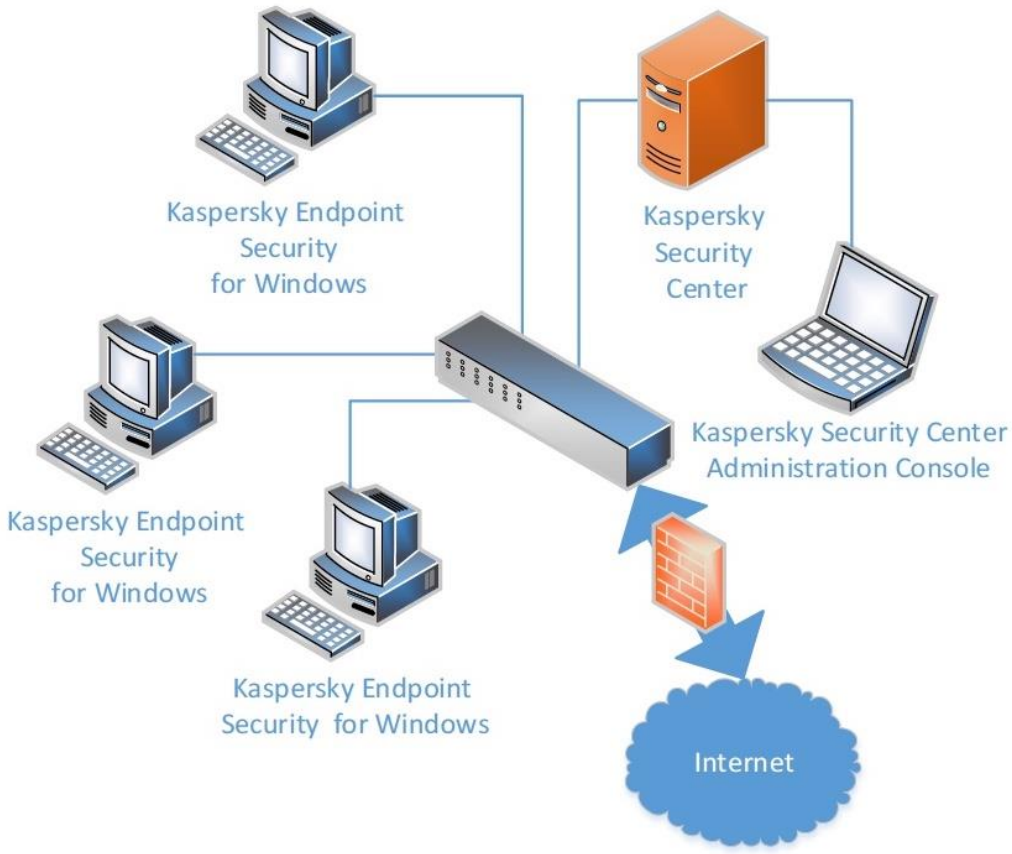

Figure 1 - TOE physical architecture

7.3.2 TOE security features

The Security Problem of the TOE, including security objectives, assumptions, threats and organizational security policies, is defined in sect. 3 of the Security Target [ST].

For a detailed description of the TOE Security Functions, consult sect. 7 of the Security Target [ST]. The most significant aspects are summarized below:

- **Full Disk Encryption Functionality**:

    1. Cryptographic Data Encryption/Master key generation: during installation of the TOE and initial encryption of the devices data (initialization), a deterministic random number generator is used for the generation of the needed AES cryptographic keys. Keys are generated by a TOE crypto library using Hash_DRBG algorithm according to NIST SP 800-90A with SHA-256.

    2. Cryptographic User key generation: during installation of the TOE and initial encryption of the devices data (initialization), a deterministic random number generator is used for the generation of the needed AES cryptographic keys (User Keys). Keys are generated by TOE crypto library by Password-Based Key Derivation Function 2 (PBKDF2) with HMAC-SHA256, 10.000 iteration value, 256-bit salt and password as input as required by NIST SP 800-132,

Option 2a. This key is later used during user authentication with username/password method.

3. Cryptographic key destruction: the TOE overwrites cryptographic keys in memory with zeros when it no longer needs them.

4. Cryptographic operations: cryptographic operations are done by TOE crypto library as required by relevant standards for the following operations: Data Encryption/Decryption, Key Encryption/Decryption, HMAC calculation, RSA Key Encryption.

5. Full Disk encryption: user data protection do not rely on OS mechanisms, that can be bypassed if physical access to disk is obtained, but on strong encryption and user authentication data.

- **Application Startup Control**: application startup control functionality of the TOE is based on filter driver interception mechanisms, where the TOE intercepts all processes being started in OS on a kernel level. When OS or application executes new application (process), the TOE scans the application being run, (or script being executed) to get process properties and metadata.

- **Device Access Control**: device control functionality of the TOE is based on filter driver interception mechanisms, where the TOE intercepts all file data operations in OS on a kernel level. When OS initiates a data transmission to or from the attached device, the TOE collects operation properties and metadata. This can be type of device, the bus or the device's individual serial number, type of operations (read or write), active user, operation time.

- **Web Access Control**: Web control functionality of the TOE is based on filter driver interception mechanisms, where TOE intercepts all data operations in OS on a kernel level. When OS initiates a data transmission to or from the network, the TOE collects operation properties and metadata. This can be type of target address, operation time, active user.

- **Identification and authentication**: the TOE performs user identification and authentication during pre-boot. User credentials are verified against stored values and disk decryption operations are available to authenticated users.

- **Security management**:

1. Security Roles: the TOE provides services to all users in the environment. The TOE has two distinct roles: KLUsers and KLAdmin. Users are associated with KLUser role when they perform authentication during pre-boot. Users are associated with KLAdmin Role when they provide valid credentials (user name and password) when prompted by the TOE when action that is restricted to KLAdmin role is initiated.

2. Management of policies security attributes: the TOE operates based on rules, access policies and other TOE data, such as KLAdmin password, encryption keys, task settings, default actions and values for Access Control Policies. All TOE policies and rules are stored in Windows registry file and are read by TOE when necessary.

- **Anti-Virus protection**:

    1. Anti-Virus Scanning: anti-virus functionality protects system from malicious software using wide range of techniques, including real-time file access monitor, on-demand on on-schedule scans of system critical areas.

    2. Anti-Virus Actions: when the AV engine provides a detection conclusion, the TOE compares received conclusion with scan settings that define possible exclusions, and actions (disinfect, delete, block, ignore) to be taken on detected objects.

    3. Anti-Virus Alerts: when a malicious object is detected and processed, the TOE generates relevant audit records, also pop-up notifications or e-mail alerts can be configured.

7.4 Documentation

The guidance documentation specified in Annex A – Guidelines for the secure usage of the product is delivered to the customer together with the product.

The guidance documentation contains all the information for secure initialization, configuration and secure usage the TOE in accordance with the requirements of the Security Target [ST].

Customers should also follow the recommendations for the secure usage of the TOE contained in sect. 8.2 of this report.

7.5 Protection Profile conformance claims

The Security Target [ST] does not claim conformance to any Protection Profile.

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3].

All the SFRs have been selected or derived by extension from CC Part 2 [CC2].

The Security Target [ST] defines the FAV (Anti-Virus) extended functional class, with the following components:

- FAV_ACT.1 (Family: Anti-Virus Actions)
- FAV_ALR.1 (Family: Anti-Virus Alerts)
- FAV_SCN.1 (Family: Anti-Virus Scanning)

For a detailed description of the extended components properties, consult section 5 of the Security Target [ST].

Please refer to the Security Target [ST] for the complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize the same objectives.

7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme Information Note [NIS3] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [ST]. Initially the Security Target has been evaluated to ensure that constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The Certification Body OCSI has supervised the conduct of the evaluation performed by the evaluation facility (LVS) CCLab Software Laboratory.

The evaluation was completed on 6 December 2021 with the issuance by LVS of the Evaluation Technical Report [ETR] that has been approved by the Certification Body on 23 December 2021. Then, the Certification Body issued this Certification Report.

7.8 General considerations about the certification validity

The evaluation focused on the security features declared in the Security Target [ST], with reference to the operational environment specified therein. The evaluation has been performed on the TOE configured as described in Annex B – Evaluated configuration. Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

The certification is not a guarantee that no vulnerabilities exist; it remains a probability (the smaller, the higher the assurance level) that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to check regularly the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the Developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [ETR] issued by the LVS CCLab Software Laboratory and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE "Kaspersky Endpoint Security for Windows (version 11.6.0.394 AES256)" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL2 augmented with ALC_FLR.1, with respect to the security features described in the Security Target [ST] and the evaluated configuration, shown in Annex B – Evaluated configuration.

Table 1 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL2 augmented with ALC_FLR.1.

Assurance classes and components		**Verdict**
Security Target evaluation	**Class ASE**	Pass
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives	ASE_OBJ.2	Pass
Derived security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.1	Pass
Development	**Class ADV**	Pass
Security architecture description	ADV_ARC.1	Pass
Security-enforcing functional specification	ADV_FSP.2	Pass
Basic design	ADV_TDS.1	Pass
Guidance documents	**Class AGD**	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life cycle support	**Class ALC**	Pass
Use of a CM system	ALC_CMC.2	Pass
Parts of the TOE CM coverage	ALC_CMS.2	Pass
Delivery procedures	ALC_DEL.1	Pass
Basic flaw remediation	*ALC_FLR.1*	Pass

Assurance classes and components		Verdict
Tests	**Class ATE**	Pass
Evidence of coverage	ATE_COV.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - sample	ATE_IND.2	Pass
Vulnerability assessment	**Class AVA**	Pass
Vulnerability analysis	AVA_VAN.2	Pass

Table 1 - Final verdicts for assurance requirements

8.2 Recommendations

The conclusions of the Certification Body (OCSI) are summarized in sect. 6 (Statement of Certification).

Potential customers of the product “Kaspersky Endpoint Security for Windows (version 11.6.0.394 AES256)” are suggested to properly understand the specific purpose of certification reading this Certification Report together with the Security Target [ST].

The TOE must be used according to the Security Objectives for the operational environment specified in sect. 4.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all the Organizational Security Policies and the Assumptions described, respectively, in sect. 3.3 and 3.4 of the Security Target [ST] are respected.

This Certification Report is valid for the TOE in its evaluated configuration; in particular, Annex A – Guidelines for the secure usage of the product includes a number of recommendations relating to delivery, initialization, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE ([KESUM], [KESUMA], [KESPP]).

9 Annex A – Guidelines for the secure usage of the product

This annex provides considerations particularly relevant to the potential customers of the product.

9.1 TOE delivery

The TOE consists of the following items:

1. The program code of the KES delivered as a binary installation package:
   `keswin_11.6.0.394_en_aes256.exe`
   SHA256 checksum: 12DBDC9014EC71BC9EF1BE884343DD5C200A662026A7EB7FB9F82E766CC7156B

2. The Application Control Plugin delivered as a ZIP package:
   `keswin_web_plugin_11.6.0.394.zip`
   SHA256 checksum: 43A8D7377CDB6130BF14E923590D3EE9291C13AE57D46F01E25DA71807CE8E3E

3. The User Manual for administering and maintaining the TOE “Kaspersky Endpoint Security for Windows. User Manual. Version 2.01”, distributed as PDF file
   SHA256 checksum: 42D8BB9C86FF8062F7B459C4F87F1EB220691C48768DA460110C8231419FEF30

4. The Addendum that references User Manual and TOE architectural evidences “Kaspersky Endpoint Security for Windows. User Manual. Addendum A. Version 2.04”, distributed as PDF file
   SHA256 checksum: 12B67ADFD1B55554A375AA9170DAE3C3B76694BAC3AD4F872E593BF9EABA641D

5. The Guide for preparing for installation and installing Kaspersky Endpoint “Kaspersky Endpoint Security for Windows. Preparative Procedures. Version 2.03”, distributed as PDF file
   SHA256 checksum: CAD0018F6279D26DD5B969C6429E85C2794D1C67EA34AFD82F75162A907DA8B0

The delivery of the TOE is secured in a manner that any user is able to determine the authenticity of the software package received. The delivery package, including the TOE and associated documentation is downloaded from Kaspersky Lab website.

All executable files of the TOE, including installation package, are digitally signed with a Code Signing Certificate with a timestamp. This allows customers to verify the origin, integrity and authenticity of the TOE. Also, the SHA256 checksums of the TOE binary files are provided to the customers to confirm that the received TOE files are the expected ones.

9.2 Installation, initialization and secure usage of the TOE

TOE installation, configuration and operation should be done following the instructions in the appropriate sections of the guidance documentation provided with the product to the customer.

In particular, the following documents contain detailed information for the secure initialization of the TOE, the preparation of its operational environment and the secure operation of the TOE in accordance with the security objectives specified in the Security Target [ST]:

- Kaspersky Endpoint Security for Windows. Preparative Procedures [KESPP]
- Kaspersky Endpoint Security for Windows. User Manual [KESUM]
- Kaspersky Endpoint Security for Windows. User Manual. Addendum A [KESUMA]

10 Annex B – Evaluated configuration

The Target of Evaluation (TOE) is the product “Kaspersky Endpoint Security for Windows (version 11.6.0.394 AES256)”, developed by AO Kaspersky Lab.

The name and version number uniquely identify the TOE and the set of its subsystems, constituting the evaluated configuration of the TOE, verified by the Evaluators at the time the tests are carried out and to which the results of the evaluation are applied.

The evaluated TOE deployment configuration includes the following elements:

- Kaspersky Endpoint Security for Windows (TOE) installed on a managed endpoint device (workstation) running Windows OS. Kaspersky Security Center 13 (Network Agent component) is also installed on this device.
- Kaspersky Security Center 13 Administration Server and Network Agent components installed on a device (server) running Windows Server OS.
- Kaspersky Security Center 13 Web Console installed on a device (workstation) running Windows OS. Kaspersky Endpoint Security for Windows management plug-in is also installed on this device.
- All devices connected to a LAN.

The TOE supports operation with the following versions of Kaspersky Security Center:

- Kaspersky Security Center 11
- Kaspersky Security Center 12
- Kaspersky Security Center 12 Patch A
- Kaspersky Security Center 12 Patch B
- Kaspersky Security Center 13

For more details, please refer to sect. 1.4.4 of the Security Target [ST].

10.1 TOE operational environment

To ensure proper operation of the TOE, the device (workstation or server) must meet the following minimum general requirements:

- 2 GB free disk space on the hard drive
- CPU:
    - Workstation: 1 GHz
    - Server: 1.4 GHz
    - Support for the SSE2 instruction set

- RAM:
  - Workstation (x86): 1 GB
  - Workstation (x64): 2 GB
  - Server: 2 GB
- Microsoft .NET Framework 4.0 or later.

Please refer to sect. 1.3.2 of the Security Target [ST] for a list of supported operating systems for workstations and servers and supported virtual platforms.

11 Annex C – Test activity

This annex describes the task of both the Evaluators and the Developer in testing activities. For the assurance level EAL2, augmented with ALC_FLR.1, such activities include the following three steps:

- evaluation of the tests performed by the Developer in terms of coverage;
- execution of independent functional tests by the Evaluators;
- execution of penetration tests by the Evaluators.

11.1 Test configuration

The Evaluators executed all the test cases on the test environment which was provided by the Developer.

The TOE test setup was prepared according to the Developer's test plan, which describes the following environment:

- Host 1:

Hardware	Software
Processor: Intel Core i3 Duo 3.10GHz RAM: 4 GB Disk capacity: 40 GB	OS: Windows 10 Enterprise 20H2 x64 Kaspersky Endpoint Security for Windows (version 11.6.0.394 AES 256) Kaspersky Security Center (version 13.0.0.11247): Administration Server, Network Agent

- Server 1:

Hardware	Software
Processor: Intel Core i3 Duo 3.10GHz RAM: 4 GB Disk capacity: 40 GB	OS: Windows Server 2016 Standard x64 Kaspersky Security Center (version 13.0.0.11247): Administration Server, Network Agent, Administration Console Kaspersky Endpoint Security for Windows management plug-in 11.6.0

Although section 1.4.4 of the Security Target [ST] contains an additional host, namely Kaspersky Security Center (Web Console), and the Developer also provided this host to the Evaluators, it was not used during the execution of the test cases because the Web Console connects to KSC and KSC could also be operated without the Web Console.

The Evaluators installed the TOE following the preparative procedures supplied in the document [KESPP]. The TOE was installed on a virtual machine, that was provided by the Developer.

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The Developer's test documentation includes a total of 104 test cases mapping the TSFIs listed in the functional specification document. The Developer also included additional test cases associated to cryptographic support SFRs.

The Evaluators found that functionalities corresponding to the TSFI-CMD (command-line interface) and TSFI-XPL (on-demand AV scan via Windows Explorer) were only marginally tested, so they focused on these interfaces during the independent testing to compensate for the incomplete coverage.

11.2.2 Test results

In the Developer's test documentation every test case has a unique test case number and a title. For each test the pre-requisites required for the test setup are included, along with detailed step-by-step instructions for execution, the expected result and the actual result.

The actual test results of all Developer's tests were consistent with the expected ones.

11.3 Functional and independent tests performed by the Evaluators

11.3.1 Testing approach

The Evaluators testing approach was to test all of the TSF of the TOE with two test cases per TSF portions.

The Evaluators selected the Developer's tests aiming to test the TOE in depth and created own test cases to further increase the tested functionalities of the TOE resulting in a more rigorous coverage.

In particular, the Evaluators performed specific tests for the following TOE functionalities:

- test of a non-malicious file for viruses;
- test of a malicious file for viruses;
- test of a malicious file for viruses from the command line.

11.3.2 Test results

The Evaluators ran all tests on the test environment provided by the Developer. The TOE test setup was prepared according to the Developer's test plan and the preparative procedures supplied in the document [KESPP].

All Developer's tests were run successfully. The Evaluators verified the correct behavior of the TSFIs and correspondence between expected results and achieved results for each test.

All test cases devised by the Evaluators passed, i.e., all the actual test results were consistent to the expected test results.

11.4 Vulnerability analysis and penetration tests

For the execution of these activities, the Evaluators worked on the same TOE test setup already used for the functional test activities, verifying that the test configuration was consistent with the version of the TOE under evaluation.

The Evaluators first performed a search of public domain sources to identify potential vulnerabilities in the TOE. This activity revealed the following potential vulnerabilities in the TLS 1.2 protocol implementation:

- The “Logjam” attack (CVE-2015-4000)
- The “Raccoon” attack (https://raccoon-attack.com/)

However, the very high complexity of these attacks would require a greater attack potential than Basic, so the above vulnerabilities are considered residual.

The Evaluators also executed the following attack scenarios:

- Testing buffer overflow in file operations from the graphical interface.
- Testing buffer overflow in file operations from the command line interface.
- Analysing a memory dump for sensitive information leakage.
- Analysing DLL files for sensitive information leakage.
- Sending an XXE attack vector as input to an import operation.

They did not result in any exploitable vulnerability.

Based on the vulnerability analysis and the penetration testing results, the Evaluators could then conclude that the TOE is resistant to an attack potential of Basic in its intended operational environment. No exploitable vulnerabilities have been identified.